Business resiliency through effective risk management

The key to managing risk lies in a resilient business infrastructure, as expounded at Cisco's event, CSO Perspectives—Strategies for Building Effective Business Resiliency

Prasanto K Roy, chief editor, CyberMedia and the moderator for the session emphasizing on the need for a clear assessment of the cost of failure to be able to determine the right approach. Sandeep Raina, senior VP, Cisco India North, and Harish Agarwal, associate director of the risk advisory practice at E&Y listen on

The ability to operate in a 24x7 paradigm is a business necessity today for enterprises. However, parallely they are faced with the business reality of a threat spectrum that is not just growing wider but also becoming increasingly more complex. Therefore, one of the biggest challenges today is managing the entire risk scenario while ensuring that their business doesn't come to a standstill. The key to this lies in building a resilient business infrastructure, as expounded during the brainstorming session at "CSO Perspectives—Strategies for Building Effective Business Resiliency" presented by Cisco. Driving home the point were a gamut of CIOs and CSOs along with some eminent security experts.

The discussions, led by the core panel consisting of Sandeep Raina, senior vice president, Cisco India North; Phaneesh Murthy, CEO, iGate; Dr Kamlesh Bajaj, CEO, Data Security Council of India; Harish Agarwal, associate director of the risk advisory practices at E&Y; and Susheela Venkataraman, who heads the strategy consulting service at Cisco, centered around building business resilience through effective risk management.

CIOs and CSOs from across the industries added the user perspective, citing the challenges being faced by them in their day-to-day operations. This included Sanjay Oswal, CTO of Bechtel; Rajiv Garg, additional GM, BHEL; Anand Kumar Pillai, senior manager, information systems at CAIRN; Dilip Barman, senior manager, network & securities, Emet India; Sachin Jain, CISO, Evalueserve; Ravi Neb, AVP, IT, iYogi; Ajay Kumar Dhir, chief information officer, Jindal Steels; KP Sapkota, manager, IT, InterContinental Hotels Group; and Kishore Ranjan, chief manager, IT, Max New York Life Insurance.

The Indian enterprises are increasingly becoming global.

Growing competition means there are new competencies that these organizations need to build and contend with new age realities like working with multiple partners, and those partners could be any where on the globe. The issues that the enterprises are looking at today are improving the ability to invent new products while moving up the value chain. Complicating it further is the fact that no longer is an organization confined to its own boundaries. Today any organization that we talk about is an eco-system. It has got its network of various partners that it works with, the customers that it works with, all of whom are increasingly getting more and more entwined with what the organization does. According to Venkataraman, all of this means that enterprises need to look at innovation, which means taking risks. "So at the end of the day when we look at building resiliency and so on, it is also about balancing risk and resilience. It is not about avoiding risk altogether. It is about looking at where do you take risks, what kind of risk do you take, and how do you balance it."

The panelists also emphasized on a proactive approach toward the business resiliency strategy. Building resiliency in an organization is not only about responding to a situation but it is also about being able to foresee. The whole issue is not whether the data is available, it is also about being able to look at the data and say, "Hey, there seems to be a trend here". And it is also about the people who notice those trends, being able to pick up the thread and say this for me signifies the fact that there is something leading up to a failure. So, increasingly organizations, when they look at their planning around risk and resiliency, have to start thinking not just about how to respond to a situation, but also about those indicators that tell them that there is something that is about to happen.

Prasanto K Roy, chief editor, CyberMedia and the moderator for the session brought up the discussion on having an integrated security plan for enterprises, which takes an integrated approach toward resiliency and business continuity. Thereby bringing to the fore the whole issue of the responsibility for driving the business continuity agenda for organizations. From the highest authority in the enterprise to the CIO, to the CSO, different organizations have followed different structure. However, there has been a growing consensus on the need for BCP to become a business driven issue, involving the business heads irrespective of who drives the business. It's a project and the business impact analysis needs to be done along with the business process owner who can understand the business very well.

Susheela Venkataraman and Dr Kamlesh Bajaj, CEO, Data Security Council of India listen attentively as Phaneesh Murthy, CEO, iGate delves on the growing expectations from CSOs today

Murthy delved on the CEOs' expectations from CSOs when it comes to security and business resiliency from the perspective of services exporters. He expounded on the expectations of CSOs to make the employees' lives comfortable by making things less cumbersome and at the same time protect the company's assets and security. He further emphasized on the need for security to be impersonal for it to be effective. On the other hand, Dr Bajaj provided the industry perspective and the road ahead for information security in India. "It's a question of people, process, and technology. There is a price to be paid for bringing security or not bringing security, and we have to identify what are the information assets that we are trying to protect in every organization so that protection has a cost to it. We need to decide how we want to actually implement this cost."

While there has been a significant change in the view of security, but what has not really changed is that majority of the enterprises have still not been able to quantify, evaluate, and get a fix on what is the cost or what is the impact of disruption of an incident. If one looks at the approach toward security, for some sectors like BFSI, telecom, IT, and ITeS where the impact is very clear. However, on the other hand, there are sectors which don't have a clear visibility into it. That is a very fundamental thing, the realization of which will gradually dawn on companies that a clear assessment of the cost of failure is going to be very critical to determine what is the approach to security, who drives it, and at what level it is driven.

—Shipra Malhotra
shipram@cybermedia.co.in